



Data protection for independent schools

Andrew Gallie - Partner

Bronwen Jones - Associate



vwv.co.uk | Offices in London, Watford, Bristol & Birmingham



Introduction



Today's topics

1. Subject access requests
 2. Complaints
 3. Accountability, documentation and training
 4. AI and data protection
 5. Personal data breaches
 6. Using and sharing personal data in practice
- ... but not the Data Protection and Digital Information Bill (RIP)

Data protection true or false

- An opinion about someone can be their personal data
- Data protection is easy, just get consent to avoid problems
- All breaches must be reported to the ICO
- “Data protection law” means the UK GDPR and the Data Protection Act
- Sharing safeguarding information can sometimes be a breach of data protection law even if it’s the right thing to do

1. Subject Access Requests



Subject Access Requests

Initial Considerations

- The right belongs to the child
- Requests from third parties
- Asking for ID
- Asking for clarification
- Calculating the deadline

Subject Access Requests

Preparing the response

- Searching for the personal data
- Social media and personal devices
- Extending the timeframe
- Applying exemptions
- Practicalities



Subject Access Requests

Other points to consider

- Refusing to respond
- Complaints to the ICO
- Reprimands and published data-sets

Case Study 1





WV

2. Complaints

2. Complaints

- Free to complain to the ICO
- Vast majority of complaints are about SARs
- ICO publishes information about the complaints it receives on its website



Dealing with complaints

- Strategy will likely depend on your relationship with the complainant
- Might need to go down official route e.g. parental complaint procedure
- ICO will usually expect you to try and resolve the complaint before they get involved (this might become law)

A blue binder with a white label that says "Complaint" is shown in the foreground. In the background, two people in business attire are blurred, suggesting a meeting or discussion. The binder is resting on a stack of papers and a folder.

Complaint

3. Accountability, documentation and training



Accountability, documentation and training

Procedures and policies

- Accountability: You must comply with the law and be able to demonstrate your compliance
- Data protection by design and default
- Not about ticking boxes
- Measures in place proportionate to the risks
- Explicitly required documents e.g. ROPA and Appropriate Policy Document

Accountability, documentation and training

Procedures and policies

- Should cover points such as:
- The essentials
- Information security
- Data breaches
- Retention
- Using photos / videos
- CCTV
- When to do a DPIA



Accountability, documentation and training

Transparency

- Privacy notices
- Age appropriate
- Layered approach
- Data collection forms

Accountability, documentation and training

Training

- Specific training for certain teams/groups
- Refresher training
- Culture and staff awareness
- All staff that handle personal data (including volunteers and governors) must have training
- Consider including a test



4. AI and data protection

AI and data protection

The basics

- What is AI?
- What sorts of things might a school use AI for?
- Will the use of AI involve processing personal data?

Case Study 2



AI and data protection – key compliance issues

- Comply with usual UK GDPR principles, e.g, around fairness
- Accuracy
- Data minimisation
- Transparency
- Security
- Check the contract with the provider
- Do a DPIA!
- Extra obligations when making important automated decisions

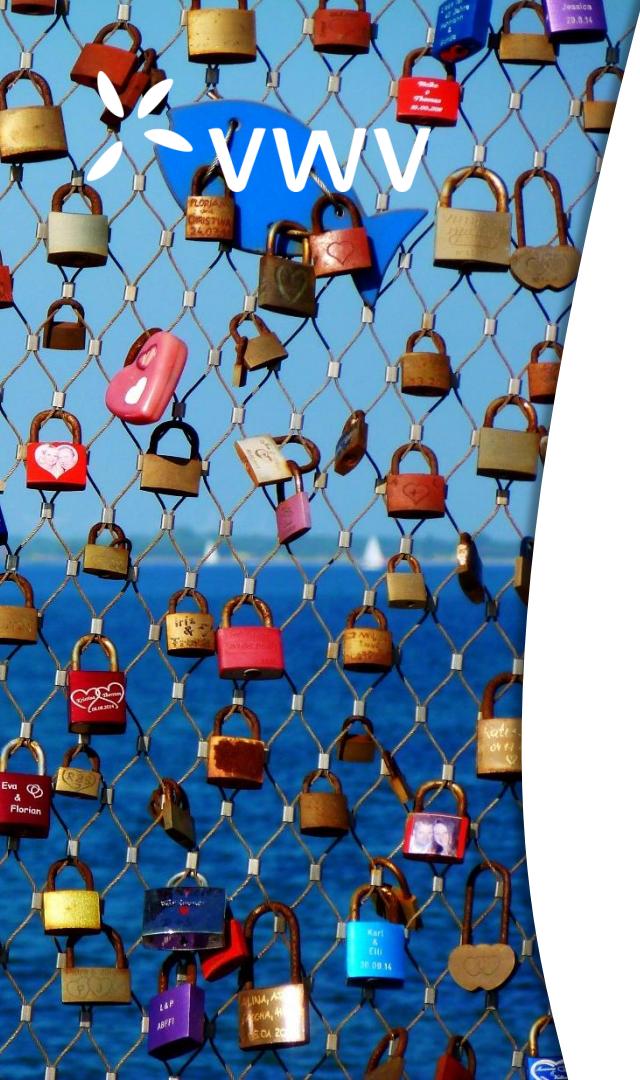




VWV

A close-up photograph of a black computer keyboard. A heavy, dark metal chain is wrapped around several keys, and a large, brass-colored padlock is attached to the chain, locking it. The keys visible include '4', '5', '6', '7', '8', '9', '0', 'E', 'R', 'T', 'Y', 'U', 'I', 'F', 'X', 'C', 'V', 'B', and arrow keys. The padlock is positioned over the 'U' and 'I' keys.

5. Personal data breaches



Personal data breaches

Examples

- Sending emails to the wrong recipient or email addresses visible to all recipients or sending the incorrect attachment
- Internal and external attacks including ransomware. E.g., ICO Interserve fine
- Misplacing paper records, e.g. during school building refurb
- Screensharing personal data by mistake
- Network security
- Data breaches caused by students



Personal data breaches

Consequences and risks

- Diversion of resource and management time
- ICO enforcement and fines
- Compensation
- Reputational damage

Data breach response

- Contain the breach
- Notify insurers
- Notify ICO?
- Notify individuals?
- Charity Commission Serious Incident Reporting
- Let the DfE know?
- Consider reporting to the police, Action Fraud and/or NCSC (National Cyber Security Centre)




Case Study 3


6. Using and sharing personal data in practice



Using images for marketing and publicity

- Should a school get consent before using images for marketing?
- Distinction between less privacy intrusive and more privacy intrusive images
- Security breaches aside, most data protection complaints seem to relate to the use of images

A photograph of a torn piece of paper with a scalloped edge, set against a brown textured background. The paper is light green and features the logo and name of the law firm Veale Wasbrough Vizards. The logo consists of three red teardrop shapes to the left of the text. The text "Veale Wasbrough" is in a large, bold, black sans-serif font, and "Vizards" is in a smaller, bold, black sans-serif font below it.

 **Veale Wasbrough
Vizards**

Sharing personal data with suppliers

- Controllers and processors. What is the difference and why does it matter?
- Most suppliers who handle school personal data will be a processor. E.g., pupil or staff IMS, some IT suppliers, payroll. A school must:
 - Do checks on the processor
 - Have a UK GDPR compliant contract in place
 - Cover any international data transfer requirements
- EdTech and data protection compliance

Sharing information with police

- No legal obligation to share unless court order
- ICO Opinion “Who’s Under Investigation?” Checklist for sharing with the police
- Police must be specific to what they want and why. They should have a request form
- Transparency
- Lawful basis and compliance generally
- Government plans to introduce new laws to clarify what police can ask for but no timeframe

Record retention

- A brief history of school record retention
- The Independent Inquiry into Child Sexual Abuse (IICSA)
- Safeguarding information: still keep indefinitely?
- What does “safeguarding” mean. Where to draw the line?
- IICSA recommendation that ICO produce new code of practice, but no timeframe



Data Protection Handbook

Key features:

- ✓ 18 policies and documents we feel are needed for data protection compliance
- ✓ Privacy notices
- ✓ Policies for all staff that contain practical guidance tailored to schools
- ✓ Policies for those with a data protection role
- ✓ Documents for compliance when using a processor e.g. template agreement

Please indicate on your feedback form if you would like to find out more.



Data Protection and Info Security eLearning

Key features:

- ✓ Practical guidance for staff reduces the risk of something going wrong
- ✓ Evidence that staff have read and understood their responsibilities
- ✓ Upload your school policy for staff to read alongside training
- ✓ Quick and easy set up

*Just **£3 per user**. Please indicate on your feedback form if you would like to find out more.*



Andrew Gallie

Partner

agallie@vww.co.uk

07467 220 831



<https://www.linkedin.com/in/andrewgallie/>

<https://www.linkedin.com/in/bronwen-jones-08b43475/>

vww.co.uk | Offices in London, Watford, Bristol & Birmingham
Lawyers & Parliamentary Agents



Bronwen Jones

Associate

bjones@vww.co.uk

07818 018 215

